AOIT Computer Networking

Lesson 8

NOS versus OS

Teacher Resources

| Resource | Description |
| --- | --- |
| Teacher Resource 8.1 | Concept Attainment: Network Operating Systems |
| Teacher Resource 8.2 | Inkshedding Stations: Types of Peer-to-Peer and Client/Server Networks |
| Teacher Resource 8.3 | Demonstrations: Access and Authentication |
| Teacher Resource 8.4 | Answer Sheet: Access and Authentication |
| Teacher Resource 8.5 | Student Roles: Client/Server Simulation Activity |
| Teacher Resource 8.6 | Short-Answer Quiz: Network Operating Systems |
| Teacher Resource 8.7 | Answer Key: Network Operating Systems Quiz |
| Teacher Resource 8.8 | Key Vocabulary: NOS versus OS |
| Teacher Resource 8.9 | Bibliography: NOS versus OS |

Teacher Resource 8.1

Concept Attainment: Network Operating Systems

In this activity, students learn about network operating systems by identifying examples of functions that an NOS can perform.

Preparation

To prepare for this activity, create two charts on the board or on chart paper. Divide the first chart into two columns with “Yes” and “No” as the headings. On the second chart, write “Characteristics” at the top—and leave room to add “Network Operating System (NOS)” above it later.

Procedure

**1. Introduction**

Tell the students they will be playing a guessing game, and when it’s over they will have created a description of a new concept. On the board, write a list of the tasks, file types, and application types that students are to categorize, for example:

* Website hosting
* Web surfing
* Word documents
* Instant Messenger
* File folders
* Company email access
* Databases
* File sharing
* Computer log-in with password (i.e., authentication)
* Roaming profiles (user can access files/settings from multiple systems)
* Microsoft Word
* YouTube

Explain any terms students might not understand. For example, roaming profiles allow workers to save their desktop remotely and secure it with a password, so that they can log in to any machine on the local network and access their same files and system settings.

On the first chart, under the “Yes” column, write two or three examples of features that require an NOS from among these examples: website hosting, web surfing, company email, databases, roaming profiles, YouTube.

**2. Pair Work**

Have students get in pairs or groups of three and make their own charts. Ask them to discuss what the given examples have in common and guess which other examples from the list fit in the “Yes” category, and why. Give them five minutes to do so.

**3. Class Discussion**

After the pair work, have students come together as a class again and have each team suggest something from their “Yes” or “No” list. Ask for a show of hands to see how many teams agree.

Write down all student guesses in the appropriate “Yes” or “No” column. Ask students to identify other examples that fall under the “Yes” or “No” column and add them to the chart. At this point you should have at least six examples in each column.

Ask students if they can figure out some of the common characteristics that apply to all of the “Yes” examples. On the second chart, list any characteristics they deduce. If students have difficulty identifying the characteristics, encourage them by providing more examples and guiding them along.

Go back and forth between the charts, adding examples and characteristics, until you’ve exhausted the lists. Explain to students that all of the “Yes” examples are things that require a network operating system. Write “Network Operating System (NOS)” above the word “Characteristics” on top of the second chart.

**4. Concept Development**

Now that students have ascertained the word for the new concept, explore its meaning and emphasize its features and functions. Discuss with students how network operating systems are different from other operating systems, particularly in how they share files and services. Then explain that the computers that use NOSs are dedicated servers. Servers can provide a variety of services for other computers on a network. Networks with dedicated servers are *client/server networks*.

Networks that don’t use NOSs are *peer-to-peer networks*. These networks consist of client computers. These client computers can also perform specific server functions if they use special server software that operates on top of the OS.

Teacher Resource 8.2

Inkshedding Stations: Types of Peer-to-Peer and Client/Server Networks

Use these sheets to set up stations where students will write what they learn about the different types of networks.

Setting Up Stations

Set up stations before class starts by hanging the information provided for each station—text and diagrams—on the walls. Also, hang a blank sheet of chart paper next to each information display.

The stations will cover the following topics (the information for each is included in the following pages).

* File Sharing in a Peer-to-Peer Local Area Network
* The Three Security Methods on a Local Peer-to-Peer Network
* Peer-to-Peer Networks on the World Wide Web
* The Client/Server Network: Dedicated Servers
* Using Server Software on a Client Computer
* Domain Controllers on Client/Server Networks
* Proxy Servers and Network Address Translation
* Domain Name System (DNS) vs. Windows Internet Naming Service (WINS)

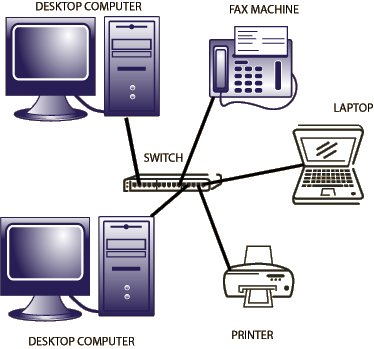
Station 1

File Sharing in a Peer-to-Peer Local Area Network

A peer-to-peer network on a LAN allows networked computers to share hard drives, file folders, Internet access, and networked resources such as fax machines and printers.

Peer-to-peer networks can be used in a small office or home office setting. They might also be used by members of a household.

For example: Students at a college dorm might plug their computers into a shared network and share music, video clips, pictures, or other files. In this way, a peer-to-peer network is sort of like a MySpace or YouTube for all sorts of files, but shared over a local network with only the people you trust, instead of the whole Internet.



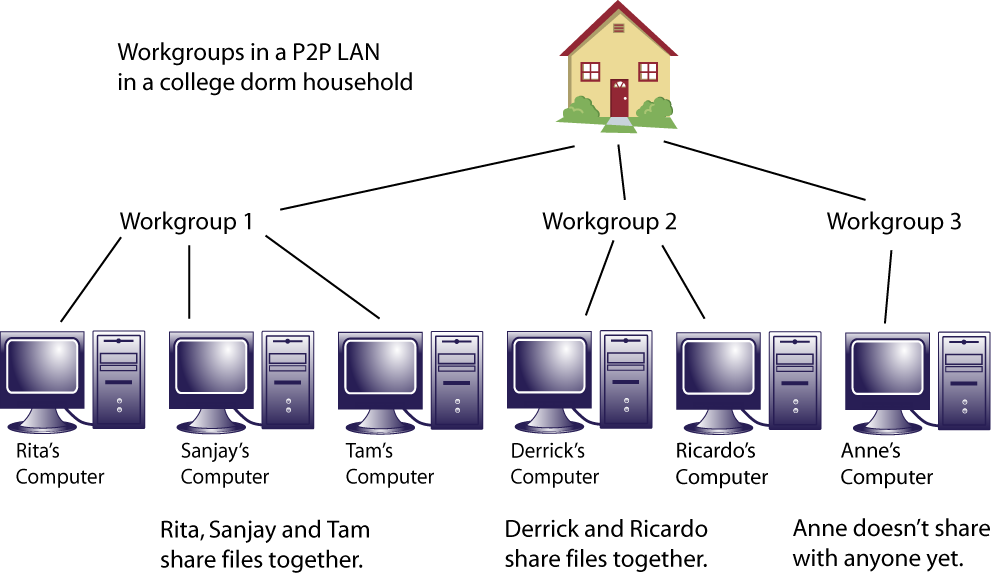
Station 2

The Three Security Methods on a Local Peer-to-Peer Network

1. Workgroups

Adding your computer to a “workgroup” allows you to share files with other computers in the same workgroup and access other folders shared by other computers in the same group.

The following shows the workgroups set up on one local area network that is used by college students who live together in the same dormitory household.



Workgroups can be password protected so that nonmembers can’t access the files. This means that Derrick can’t see Rita’s shared folders, because they don’t share a workgroup. No one can access Anne’s files, either, because she has her own workgroup.

2. Passwords

In a workgroup, file security is the responsibility of the end user. Users can set access rights to specific files and folders, using the login password for their local workstation.

3. Permissions

Using permissions, you can decide how much control others have over your shared documents. There are three essential levels of file permissions you can set:

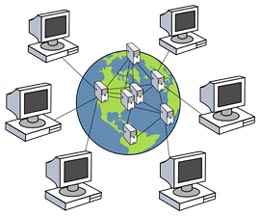
* **Read Only:** Other users can see the document, but they can’t edit it.
* **Write Only/Change:** Users can read, edit, or add to the document, but they can’t delete the file.
* **Read & Write, or Full Access:** Users have full control, and they can edit or delete the document.

Station 3

Peer-to-Peer Networks on the World Wide Web

If you’ve downloaded music from Napster or LimeWire, or movies from BitTorrent, you have used a peer network across the web. Here are some features of peer-to-peer networks on the web:

* Anyone who has the right software can connect to the network, from anywhere in the world.
* You select which folder to share with other people, and add files you want to share.
* You can search other people’s folders for files they have shared.
* The program sets up a direct connection between the two computers transferring data.
* Security is really limited—many people share dangerous files on the web, to get you to download programs that can do your computer harm.
* Criminals have used peer-to-peer networks to download other people’s tax forms or other important documents. They use the stolen information to commit fraud and theft. So be careful what you share!



If you use these networks, be careful! Follow these guidelines to protect yourself and your computer:

* Most important: Check the size of any file you want to download. If the size is different from what you expect it to be, it might be damaged or corrupted—or it might be a malicious software file that can hurt the computer.
* Share only a small number of files and don’t share any that contain information about yourself.
* If it’s a music file, preview during download to make sure it’s what you expected.
* Cancel anything that says it’s corrupted or damaged.
* Check the user agreement on the client program (Kazaa, etc.) to make sure it doesn’t include adware and spyware with the application. If it collects a lot of information about you, it’s not worth it.
* If you start getting pop-up ads, stop using the program and uninstall it.

Station 4

The Client/Server Network: Dedicated Servers

Every client/server network has at least one computer that works only as a server. You wouldn’t log in and start typing an essay or browse the Internet on that computer. But it does perform important functions for other computers on the network.

Servers run a network operating system like Windows Server 2003 or Windows Server 2008. Some might also run Linux or Unix.

Types of Servers

Here are some examples of types of servers:

* **Domain controller**: This type of server stores information about people who use the network. Such information includes user names, passwords, system settings (like the user’s desktop background), the applications the user can access, and the documents she creates or edits. This type of server is a Microsoft Windows server and doesn’t apply to Linux or Unix.

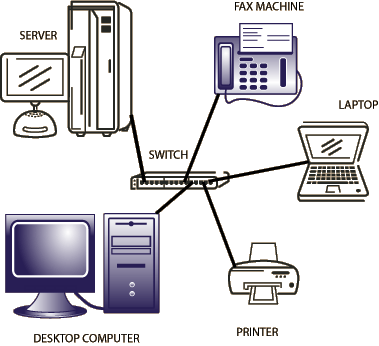
A domain controller saves all this information centrally. So, users can log in to any computer on the network with their unique user name and password and access all of the files and everything listed above.

* **Web (HTTP) server**: A web server stores the files, images, and file folders for a website so that other computers can see the site.
* **Email server**: An email server controls how emails are received, filtered, stored, and sent on a company network.
* **Proxy server**: A proxy server controls the entrance to a network from the outside Internet. It also is usually responsible for controlling IP addresses.
* **File server**: File servers store databases or file folders of documents that many different people on the network need access to. A client computer can access these files if its user enters the right password and it is allowed access.
* **Application server**: This type of server stores the software programs that all the client computers use. Instead of Microsoft Word being on your desktop, it would exist on the server machine and your client computer would use it remotely.

On small networks, one server might perform a few or all of these functions.

On larger networks, there might be one server for each function!

Simple Client/Server Network with One Dedicated Server

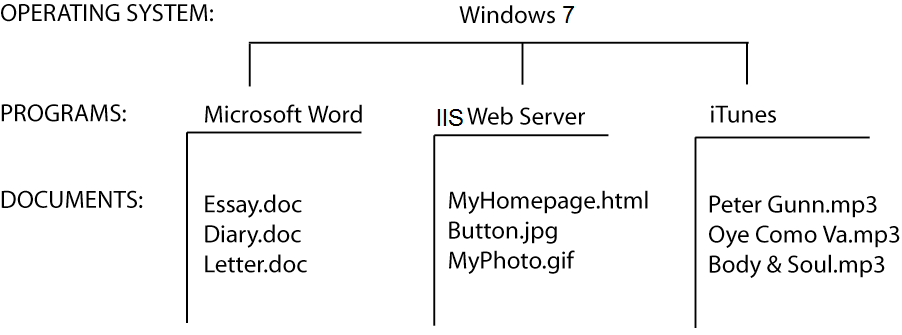


Station 5

Using Server Software on a Client Computer

Say you want to host your own website from your home computer. You want to continue to write essays, browse the Internet, and do everything else you normally do on the computer. But you also want the computer to work as a server and supply files to other computers that want to view your website.

You don’t have to run a full server platform with a network operating system to do this. You can use the operating system on your computer, such as Windows 7 or Windows XP. You will also need to install server software that can perform the specific function you need. Then your computer can function as a client computer, to perform all your normal tasks, and also as a server. You will have a computer that functions both as a client and as a server.



IIS (Internet Information Services)

IIS is the web server that is packaged with most editions of Windows. You can install it on your computer in order to host your own website. For instructions on how to install IIS on a Windows 7 system, for example, visit the IIS website at <http://learn.iis.net/page.aspx/28/installing-iis-7-on-windows-vista-and-windows-7>.

Station 6

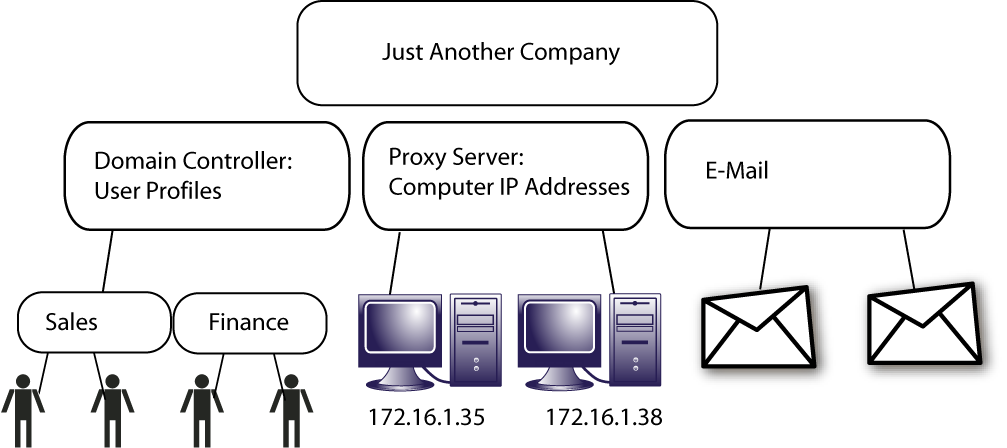
Domain Controllers on Client/Server Networks

A domain controller is a database that stores profiles for all of the network’s users. It’s one of the simplest but most important functions of a server.

The profiles might include:

* Login names and passwords
* System settings, permissions, and preferences
* Applications the user can access
* File folders and documents

The information is stored on a central server so that users can log in to any computer on the network and access their information and files. This ability is called “roaming authentication.”



The diagram above shows how different addresses are stored separately on company servers. The domain controller stores user profiles. These are separate from the computers’ IP addresses, which are assigned by a proxy server. And the users’ email address accounts are stored on a mail server.

In some networks, one server might perform all of these different functions. But the user profiles are still stored separately from IPs and email accounts.

Domain Controllers with Active Directory

Windows Server 2003 and Windows Server 2008 use a service called **Active Directory**, which blurs the line between the primary and backup domains. Active Directory stores profiles for all users on all the computers on the network, and profiles are updated all the time. So if the server fails, the user profiles are not lost.

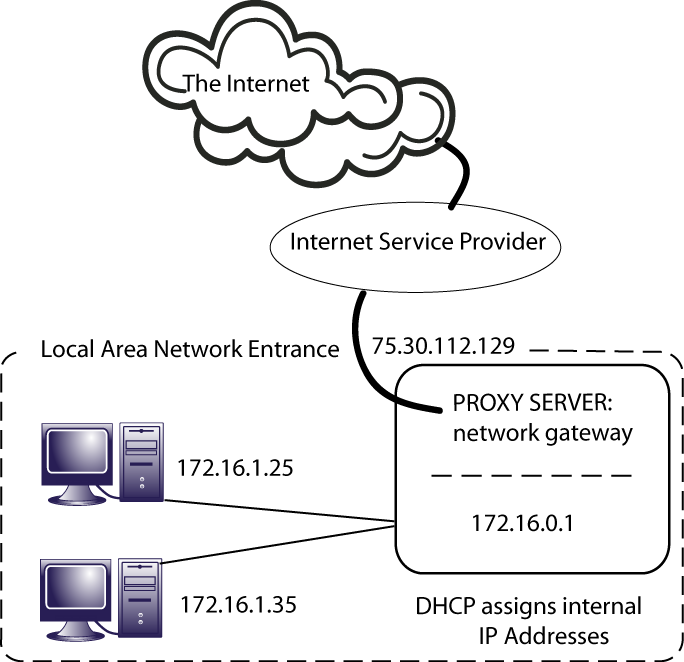
Station 7

Proxy Servers and Network Address Translation

The proxy server is the LAN gateway—it functions as the entrance to a local area network (LAN) from the Internet.

The server protects the internal network by using two separate IP addresses: a public address that the Internet can see and a private one used on the local network.

The Internet service provider (ISP) assigns the entire local network one or more unique IP addresses. But the network’s computers still need a way to route messages to each other internally. So, the proxy server, using DHCP (Dynamic Host Configuration Protocol), also assigns a different IP address to each of the computers on the network.



Network Address Translation (NAT)

Since the router has two IP addresses—one for the Internet and another for the local area network (LAN) —it has to translate between them when traffic travels from inside the LAN to outside, on the Internet. This process is called “network address translation.”

The gateway (or proxy server) assigns itself an internal address and uses DHCP to automatically assign IP addresses to each computer on the internal network. All the computers’ internal IP addresses are hidden from anyone outside the local area network. The whole LAN looks like one machine to anyone on the Internet because it is represented by only one IP address.

This setup has two benefits:

1) Different local area networks can reuse the same internal IP addresses.

2) The computers on the network are more protected and secure.

NAT Improves Security

Network address translation helps to filter traffic coming into the network.

* It is one kind of firewall that can filter traffic based on IP addresses.
* It can block some pop-ups and spam from coming into the network.
* Additionally, all the messages that leave the network look like they are coming from the gateway server, not the internal computers.

Station 8

Domain Name System (DNS) vs.   
Windows Internet Naming Service (WINS)

Associating Names with IP Addresses

On the Internet, DNS stores the names for websites like Google.com or Wikipedia.org and the web addresses that are linked to them. When you type in “Google.com,” DNS translates that name into an IP address and finds the web host that stores the Google web files based on that address.

On a LAN using DHCP, the same feat is accomplished using Windows Internet Naming Service (WINS), which uses NetBIOS names for individual computers, like “Laura’s Computer.”

|  |  |
| --- | --- |
| Domain Name System (DNS)  * **Used on the Internet** * **Example:**   **Domain Name:** www.google.com  **IP Address:** 64.233.167.99 | Windows Internet Naming Service (WINS)  * **Used on a local network** * **Example:**   **NetBIOS Name:** Laura’s Computer  **IP Address:** 172.16.1.15 |

Why Use DNS or WINS Instead of IP Addresses?

* It’s easier to remember a name like Google than the address 64.233.167.99.
* Remembering a site’s name rather than its IP address is more fun, too!

Teacher Resource 8.3

Demonstrations: Access and Authentication

Using a computer and an LCD projector, perform the procedures outlined below as students follow along on their own computers. Refer to Teacher Resource 8.2 for additional information about each demonstration.

Activities

File Permissions in Peer-to-Peer Networks

Lead students through the process of viewing and changing file permissions in peer-to-peer networks. Explain that students can decide which folders to share and the level of permission they want to grant other users. They can share the whole drive or just specific folders. They can assign Read Only, Write Only/Change, or Full Access, depending on how much control they wish to give to other users.

Show students where they will be able to view and change these permissions on the computer.

First, if using Windows XP, turn off simple file sharing to enable full control over who views files. Go to My Computer, and in the Tools menu, click Folder Options. In the dialog box that appears, select the View tab. In the Advanced Settings section, make sure “Use simple file sharing” is **not** selected.

Then, to configure file sharing, students can right-click a folder and select Properties, and then the Sharing tab. To share files, students will need to select “Share this folder,” then supply a name by which the folder can be recognized on the network. Here they can also enter a maximum number of users allowed to view the file at once.

To set restrictions and limitations of the permissions, students can then select the Security tab.

In the box that appears, they can select Add to find users or groups with whom to share files, or click Remove to select a group they do not want to share files with.

Then, for each group, students can assign varying levels of permissions, which function as variations on the following:

* Read Only: You want your friend to read a poem you wrote but not to make any changes to your work.
* Write Only/Change: You want a friend to help edit your essay but you don’t want her deleting it.
* Full Access: Your friend wrote an essay on your laptop computer, so now you want to share it with him and grant him full access to make changes or delete it.

**Note**: If teacher and student computers are blocked and you cannot access file sharing, there are other options:

* Connect two computers with a crossover cable.
* Use a computer that is not connected to your school’s network and show students the various settings using an LCD projector. You do not need a computer that has Internet access.
* Ask students to take some notes on file sharing and try looking at the menus on their home computers. Remind them that Internet access is not necessary.

Roaming Authentication on a Client/Server Network

In Inkshedding Station 6, students studied how domain controllers allow user profiles to be stored on a central server so that users can log in from any client machine. Show students the diagram from that station again, to illustrate how user profiles and other documents are stored separately.

Storing everything on central servers means that users don’t have to be tied to one client computer to access their information. All their user information, such as login name and password, documents, system settings, and preferences, are stored in a domain controller. If they are used to working at one desk but that computer fails, they can simply go to another cubicle and work from a different computer by logging in to the server with their login and password.

When accessing files from the web, you are also using client/server networks. The computer and the web browser it uses to access a website are the clients, in this case. (Clients can be the user, the software, or the computer itself.) The website is stored on a server. When you visit a website, the client is retrieving the web page files from a server on the Internet, as it would from an intranet on a local network.

Have students load a web browser and log in to an online account such as their Yahoo! mail, Google mail, or MySpace account. These logins are what is called “authentication.”

Ask students whether they can also access these accounts from another computer at home, in the school library, or at a friend’s house. Explain that this is an example of what is called “roaming authentication,” because you can authenticate from many workstations, or “roam.” Students may be familiar with the concept of roaming from their cell phone usage. Roaming is also used in cellular networks to authenticate your phone number on another provider’s network.

In large companies, administrators use roaming authentication to control user access to shared folders and applications within the company network. The local area network using a client/server network is called an intranet, *intra* meaning “inside.” *Inter,* from Internet, on the other hand, means “existing between” and suggests connection—the connection of many LANs, in the case of Internet; the word being related to *intertwine*, an *interstate* highway, or *intermediate*.

Mapping a Shared Drive—File Sharing on a Client/Server Network

In a peer-to-peer network, if someone shuts his computer down, his files will no longer be available for others. One benefit of using a client/server network is that files will always be available so long as the server is running.

Shortcuts make it easier to share files—you don’t need to memorize the list of embedded folders that a certain document is stored on.

When working off a server, you can also mount a shared network drive, so that it shows up under My Computer as if it were on the local machine. This is done by assigning a drive letter to the shared drive. The main hard drive’s letter of any computer is usually C, and additional ones might be assigned as D, E, or any others. When the letter appears with the network drive, it is “mapped” to the drive.

Here are the steps for mapping a network drive:

1. Open the Windows Start menu and find My Computer.
2. Select the Tools menu and click Map Network Drive.
3. In the window that opens, select the drop-down list next to “Drive:”
4. Any drives that have already been mapped will show the folder name in the list. Select a drive letter that hasn’t been assigned yet.
5. Click the Browse button to find the shared network folder that you want to map.
6. If you want the computer to always recognize that drive, select “Reconnect at login.” Otherwise, the drive will be only temporarily connected while the user is logged in.
7. Click Finish.

Troubleshooting:

* If the disk letter was previously assigned to a different folder, a dialog box will ask whether you wish to disconnect the previous mounted drive.
* If it cannot be mapped, make sure the folder name is spelled correctly and correctly set up to be shared, and that the correct user name and password have been entered.
* To disconnect: Select My Computer >Tools and click Disconnect Network Drive.

More Information: How Permissions Work in a Client/Server Network

Since user profiles are stored separately from the computers and files, different types of permissions can be set for different users, and users can belong to different types of groups.

For example, a company’s Accounting department might have access to a network drive for all accounting-related files, such as spreadsheets, financial applications like QuickBooks, and so on.

Meanwhile, the Marketing department doesn’t need to see those resources, so they can’t log in to those drives. Instead, they can access the Marketing department folder, which contains the documents they do need to see, such as archives of advertisements, drafts of current brochures or newsletters, and graphic design software like Adobe Creative Suite.

However, in a server network, including users in one group doesn’t exclude them from another group. So, managers of both Accounting and Marketing can also be allowed to see the contents of another folder, titled “Confidential.” This folder might contain important information about the company’s high-level plans that the lower-tier staff doesn’t need to know.

Using Ping and Nslookup to Learn about DNS

In Inkshedding Station 8, students read about DNS, which catalogs and stores the links between a domain name on a network or the web (such as Amy’s Computer, or Google.com) and its host IP address. Remind students that DNS is the Domain Name System that keeps track of these name-to-number conversions and stores the information.

You can use the ping and nslookup commands as described below to find IP addresses, but note that if the administrator has blocked ICMP packets on your school network, ping and nslookup will not work.

Have students open the command prompt on their computers. Tell them there are a couple of ways they can find the IP addresses of common domains.

One way is to use the ping command. On the command line, students can type ping cuteoverload.com (or use another popular website). Point out how they can type in the domain name, but the computer recognizes it as an IP number and shows them the address as it sends packets. Ping is a troubleshooting tool to check that the Internet connection is active and that the packets can be sent and received in a timely fashion.

Another useful command is nslookup, which tells the server name as well as its IP address. Have students typenslookup ebay.com at the command line. The first address returned is the proxy server name and address. Then the command also returns the domain name and host IP address.

**Note**: If your student computers cannot access the command line, you can complete this activity by entering the command line prompts on your computer and then either displaying the transaction to students using an LCD projector or having students gather around your computer.

Using Ipconfig to Learn about NAT and Subnets

In Lesson 6, students used the ipconfig command to find their computer’s IP address. Now they can type the ipconfig command again and take a deeper look, to learn other important IP addresses on their network.

One example is the subnet mask. Explain that in a large or complex network, the network can be made both more secure and more efficient by assigning subnet masks to different departments or sections on the network. This adds another address to a portion of the network. The subnet is like a ZIP code or the name of a specific neighborhood in a larger city. All the subnets appear to be one network to the outside world.

This brings us to network address translation (NAT), which students read about at Inkshedding Station 7.

Tell students that the way NAT works on the gateway is like two sides of the classroom door that leads in from the hallway. An identifying number or poster on the door is visible to anyone in the hall, but those inside the hall cannot see the inside of the door.

With the ipconfig/all command, students can see the internal, local IP address of their gateway router and DHCP server, which is like seeing what is inside the door. Then they can visit the website <http://www.dslreports.com/whois>, which shows the IP address that is beyond, broadcast from the local network to the Internet.

**Note**: If your student computers cannot access the command line, you can complete this activity by entering the ipconfig/all command on your computer and then either displaying the transaction to students using an LCD projector or having students gather around your computer.

Teacher Resource 8.4

Answer Sheet: Access and Authentication

Use this answer sheet as a guideline for how students should fill in the worksheet.

|  |  |  |
| --- | --- | --- |
| Activity Name | Type of Network  (Peer-to-Peer or Client/Server) | Activity Description |
| File Permissions | Peer-to-Peer | Editing file access and permission settings for documents |
| Roaming Authentication | Client/Server | Accessing server accounts through a roaming profile |
| Mapping a Shared Drive | Client/Server | Mapping a shared network drive to appear on the local computer |
| Using Ping | Client/Server | Learning the IP address for a popular domain name, to see how they are connected  Learning how ping can be used in troubleshooting |
| Using Nslookup | Client/Server | Looking up the IP address and server name for a given domain name |
| Using Ipconfig | Client/Server | Viewing ipconfig addresses for router and subnet mask, and comparing them with Whois information to see how the internal address differs from what is being broadcast to the Internet |

Teacher Resource 8.5

Student Roles: Client/Server Simulation Activity

Cut out the role-play strips (1–6) in this resource and distribute them, one to each group of students.

|  |  |  |
| --- | --- | --- |
| 1 | Who am I?  A desktop computer at 172.16.1.35. Your user name is Networking and password is C0mput3rs. | What is my job?  Print a copy of MyReportCard.doc off of your shared file server. |
| 2 | Who am I?  A desktop computer at 172.16.1.25. | What is my job?  Retrieve the National Academy Foundation website at www.naf.org. |
| 3 | Who am I?  A laser printer at 172.16.1.28. | What is my job?  When you get a request from the print server, 168.0.15.5, check to make sure you have paper. Then print documents. |
| 4 | Who am I?  A web server on the Internet, at www.naf.org or 208.68.173.167. | What is my job?  Host the National Academy Foundation website files.  When a request comes in, send back the status line “HTTP/1.1 200 OK” along with your message or files in response to the request. |
| 5 | Who am I?  A LAN gateway router with a local address at 168.0.0.1 and an Internet address at 66.235.202.61. | What is my job?  When you receive a request from a local computer, direct it to the proper address. If it starts with 168 or 172, you know it is on the local network. If it is another address, you know it is on the Internet. To send an Internet request, you must use network address translation.  First, log which computer on the network sent the request to you. Then change the addresses on the message so that it shows the origin address as your network’s Internet address, 66.235.202.61.  Send the message along. When you get a reply back, check your log to see which local computer sent the request, and forward the reply to that computer. |
| 6 | Who am I?  A LAN file and print server at 168.0.15.5. | What is my job?  You store files on the local network and share them with users, but only those who have a password. The password is C0mput3rs. |

**Note:** You may consider adding one more to this list: a proxy server. The person representing the proxy server would be very “nosey,” standing near the door and deciding who can enter based on the message the person carries. A router can filter based only on IP address or where a message comes from, but a proxy server can filter based on a message’s contents.

Teacher Resource 8.6

Short-Answer Quiz: Network Operating Systems

1. Explain what kind of network workgroups are used in and how they help users share files.
2. What are two differences between sharing files in a peer-to-peer LAN and using a peer-to-peer file sharing client like Napster on the Internet?
3. What are some of the roles a dedicated server might play in a client/server network?
4. What kind of network uses roaming authentication, and how does it work?
5. Briefly describe how network address translation hides the addresses of computers on a local area network from computers on the Internet.
6. What is the Domain Name System (DNS) on the Internet, and what is the comparable service within a LAN?
7. What does it mean to map a shared drive in a client/server network?
8. What information can you learn from using the ipconfig command at the DOS prompt?

Teacher Resource 8.7

Answer Key: Network Operating Systems Quiz

1. Explain what kind of network workgroups are used in and how they help users share files.

Workgroups are used on peer-to-peer networks. Each computer joins a workgroup, and users can easily share files with the other computers in their workgroup.

1. What are two differences between sharing files in a peer-to-peer LAN and using a peer-to-peer file sharing client like Napster on the Internet?
   * One is local and one is global.
   * Peer-to-peer file sharing on a LAN uses shared file folders and settings configured in the operating system, while sharing on the web requires a special software client like Napster, BitTorrent, etc.
   * Passwords and permissions can be set in the LAN, but on the web, everything in the shared file is shared with other users.
   * In the LAN, you can see the names of people’s computers and workgroups, but you don't see the names of users on the web. (However, in peer-to-peer file sharing, your computer IP address can be traced back to you—as the RIAA and MPAA lawsuits have demonstrated.)
2. What are some of the roles a dedicated server might play in a client/server network?

A dedicated server might function as a domain controller to store an Active Directory of user profiles, or as a proxy server, an email server, a web server, an application server, a file server, a print server, or a database. A dedicated server might serve multiple functions in a small network.

1. What kind of network uses roaming authentication, and how does it work?

A client/server network can use roaming authentication to verify users’ identities when users log in to the client computers. The server provides a domain controller, which stores user profiles such as login and password. The server requires people who want to access the client computers to authenticate themselves by providing their user name and password. Since the information can be accessed remotely, this allows people to log in to their profile from any client machine on the network—hence the term roaming authentication.

1. Briefly describe how network address translation hides the addresses of computers on a local area network from computers on the Internet.

A gateway router possesses two IP addresses: one visible to the local network and one visible to the Internet. Computers on the local network see the internal address and each others’ IP addresses. Computers outside the network see only the gateway’s external address. When traffic leaves the local network, the gateway hides the internal addresses by representing the whole local network with its external IP address.

1. What is the Domain Name System (DNS) on the Internet, and what is the comparable service within a LAN?

DNS stores the information relating a web host’s IP address to its domain name, such as Google.com, on the web. This makes it easier for users to remember where to find a given web domain. On the local network, Windows machines use Windows Internet Naming Service, or WINS, to assign a NetBIOS name to a host computer.

1. What does it mean to map a shared drive in a client/server network?

A drive that stores files on a server can be mapped to a local computer by assigning the drive a local drive letter. Doing so provides a shortcut from the local computer to the remote host server and makes the drive appear to be stored on the local computer.

1. What information can you learn from using the ipconfig command at the DOS prompt?

ipconfig can reveal a local network’s IP address configurations for the devices attached to the network—such as client computers, the gateway router, and printers or fax machines—as well as for the subnets.

Teacher Resource 8.8

Key Vocabulary: NOS versus OS

These are terms to be introduced or reinforced in this lesson.

| Term | Definition |
| --- | --- |
| Active Directory | A Windows database used to store information about users, such as their user names, passwords, and system preferences, and the shared resources they are authorized to use. |
| authentication | The login process used to ensure that a user is who he claims to be and should be granted network access. |
| authorization | The process of granting or denying access to specific network resources based on the user’s identity. |
| centralized | A client/server network is a centralized system, meaning the server provides resources in one central location for other remote computers to access. |
| dedicated server | A computer used exclusively as a network server, providing shared network resources or performing network tasks. |
| domain controller | A basic type of Microsoft Windows server that stores user profiles and controls user authentication and security on a client/server network. |
| Domain Name System (DNS) | An Internet service that translates domain names (such as www.google.com) into IP addresses. Networks rely on numeric values, but domains are easier for humans to remember. |
| drive mapping | The process of creating a shortcut and assigning a drive letter to a shared network drive, so that the drive appears to be located on the local computer. |
| host | A computer system that stores files or information for other computers to access via the network—such as a web host that stores website files, or a client sharing files on a peer-to-peer network. |
| ipconfig | A command used to display the IP addresses for the local network, including the computers, routers, subnets, and more. |
| network address translation (NAT) | An Internet standard that enables a router to use one IP address for external (Internet) traffic and a separate one for internal (LAN) traffic. |
| network operating system (NOS) | An operating system used by a server; provides capabilities beyond a regular operating system to run a client/server network. |
| nslookup | A command for diagnosing DNS problems. When a network is functioning properly, using nslookup for a web domain will display the host server, its IP address, and the address associated with the domain name. |
| permissions | In a peer-to-peer network, files can be shared with one of three permission levels: Full Access, Write Only/Change, or Read Only. Files can be password protected. |
| ping | A command used at the command line to test the speed of a connection to another computer or website. |
| proxy server | A proxy server sits at the edge of the local network and connects to the Internet. It uses network address translation to make it appear as if all LAN traffic has originated at the gateway IP. |
| roaming | The capability of logging in to a network from multiple locations. In local area networks, it means that user information is stored on a network server, and users can access their system preferences and files and access shared resources from multiple client workstations. |
| segment | One section of a local area network, separated from other segments by bridges, routers, or switches. Subnets can also segment networks. Segmenting a large LAN is useful for keeping most network traffic within its own segment, to speed up the network overall. |
| subnet | A portion of a network sharing the same part of an IP address. |
| user profile | A profile containing desktop settings, preferences, and so on that Windows uses to keep track of users. |
| web server | A server that hosts a website or other files and is available for computers on the Internet or intranet to access. |
| workgroup | Client systems on a peer network can join a workgroup to share files with other systems in the same group. |

Teacher Resource 8.9

Bibliography: NOS versus OS

The following sources were used in the preparation of this lesson and may be useful to you as classroom resources. We check and update the URLs annually to ensure that they continue to be useful.

Print

Lowe, Doug. *Networking All-In-One Desk Reference for Dummies,* 2nd ed. Indianapolis, IN: Wiley, 2005.

Online

Becker, Ralph. “IP Addressing.” IP Address Subnetting Tutorial, <http://www.ralphb.net/IPSubnet/ipaddr.html> (accessed May 21, 2012).

“Domain Name System.” Wikipedia, <http://en.wikipedia.org/wiki/Domain_Name_System> (accessed May 21, 2012).

“Hypertext Transfer Protocol.” Wikipedia, <http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol> (accessed May 21, 2012).

Lane, Victor. “TCP/IP and Networking Tools.” The Command Line in Windows, <http://commandwindows.com/tcpiputil.htm> (accessed May 21, 2012).

Mitchell, Bradley. “How to Map a Network Drive in Windows XP Using Windows Explorer.” About.com, <http://compnetworking.about.com/od/windowsxpnetworking/ht/mapnetworkdrive.htm> (accessed May 21, 2012).

Tyson, Jeff. “How Network Address Translation Works.” HowStuffWorks, <http://computer.howstuffworks.com/nat.htm> (accessed May 21, 2012).